BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-203

15 AUGUST 2001

Security

SECURITY FORCES MANAGEMENT INFORMATION SYSTEM (SFMIS)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: HQ AFSFC/SFOP (Mr. Ken Saxon)

Certified by: HQ USAF/XO
(Lt Gen Robert H. Foglesong)

Supersedes AFI31-203, 18 December 2000

Pages: 9
Distribution: F

This instruction mandates the use of the Security Forces Management Information System (SFMIS) for all active duty, reserve and guard security forces units. SFMIS is the replacement program for the legacy system, Air Force Security Police Automated System (SPAS). SFMIS will provide a subset of functions with improved data quality, provide a centralized function to support MAJCOM and Air Staff needs, and comply with DOD's mandated Defense Incident Based Reporting System (DIBRS) (DODD 7730.47 *Defense Incident Based Reporting System*,and DOD 7730.47-M *Manual for Defense Incident-Based Reporting System.* SFMIS will result in an integrated combat support information system that is responsive to Air Force needs during wart and peacetime operations. SFMIS was developed by HQ Standard Systems Group (HQ SSG), Maxwell AFB-Gunter Annex AL and Scientific Applications International Corporation (SAIC). The system provides for a preset query and analytical capability at all user levels (HQ USAF, HQ AFSFC, MAJCOM, and base level). This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10 USC Section 8013 and Executive Order 9397, 22 November 1943, System of Records Notice, F031 AF SP E applies. Maintain and dispose of all records created as a result of prescribed processes in accordance with AFMAN 37-139, "*Records Disposition Schedule.*"

SUMMARY OF REVISIONS

This interim change (IC) 2001-1, mandates all security forces units accomplish a monthly computer run within the "Criminal Summary Report" section to identify criminal activity to be reported to the Air Force Office of Special Investigations (AFOSI) for DCII data inputs. It also mandates the use of the AF Form 3545, Incident Report, to document all incidents reportable under the purview of the Defense Incident-Based Reporting System (DIBRS). A (|) indicates revision from the previous edition.

Chapter 1

POLICY AND PROGRAM MANAGEMENT

1.1. Background.

1.1.1. The Security Forces Management Information System (SFMIS) automation system was primarily developed to meet the Congressionally mandated Defense Incident Based Reporting System (DIBRS) requirements and improve day-to-day operations of the Air Force security forces, as well as fulfilling the problem solving and decision making information needs of HQ Air Force Security Forces center (AFSFC), Major Commands (MAJCOMS), and their security forces units.

1.1.2. The SFMIS complies with DIBRS reporting criteria and offers all management levels the capability to monitor and apply law enforcement selective enforcement measures to meet their specific needs and perform data analysis for law enforcement statistics. Future applications will be added to SFMIS to assist management and improve security forces functions.

1.1.3. Future applications to SFMIS will be introduced through an approved HQ Air Force Security Forces Center and MAJCOM Configuration Control Board action.

1.2. Defining Responsibilities.

1.2.1. The Office of Under Secretary of Defense for Personnel and Readiness (OUSD (P&R)) develops overall policy for DIBRS and monitors compliance. They direct that a central repository of incident-based statistical data be maintained at the Defense Manpower Data Center (DMDC) for analyzing trends in response to executive, legislative, and oversight requests for statistical data relating to criminal and high-interest incidents.

1.2.2. DMDC formulates a data collection mechanism to track and report DIBRS information from initial contact through investigation, prosecution, confinement and release, and to report National Incident-Based Reporting System (NIBRS) data (extracted and reported by DMDC) to the Federal Bureau of Investigation (FBI).

1.2.3. As each security forces unit becomes SFMIS operationally capable of reporting, each active, reserve, and guard Security Forces unit will use SFMIS and comply with the reporting requirements as mandated by Congress and outlined in DODD 7730.47, *Defense Incident Based Reporting System (DIBRS)*, and DoD 7730.47-M, *Manual for Defense Incident-Based Reporting System (DIBRS).*

1.2.4. Criminal Activity Reporting. The Air Force SFMIS fully supports the requirement to report criminal activity in response to Section 534, United States Code, "*Uniform Federal Crime Reporting Act*", Section 10606 and 10607, of Title 42, United States Code, "*Victims Rights and Restitution Act of 1990*", and Section 922, United States Code, "*The Brady Handgun Violence Prevention Act*".

1.2.5. HQ Air Force Security Forces Center, Police Services Branch, is the focal point for all issues pertaining to DIBRS reporting requirements and other reports and analysis statistical data. Once a month, HQ AFSFC/SFOP will report DIBRS data to the DMDC.

1.2.6. MAJCOM Responsibility.

1.2.6.1. Each MAJCOM/SF will appoint a system administrator (SA) who will act as the grantor of permissions and accesses for each of their respective units within their command. It is advisable to appoint an alternate SA.

1.2.6.2. When requested by higher headquarters, each MAJCOM will send a representative(s) to the Configuration Control Board (CCB) meetings which are empowered to identify and define current and future SFMIS requirements. Once requirements are mandated, with the assistance of HQ SSG, an Operational Requirements Document will be developed and will serve as the Statement of Work (SOW) for the project(s).

1.2.7. Security Forces Unit Responsibility.

1.2.7.1. Each Security Forces Unit Chief will appoint a System Administrator (SA) at their respective location who will act as the grantor of permissions and accesses for personnel requiring access to SFMIS in the performance of official duty. It is advisable to appoint an alternate SA. Internal controls will be established to allow management to view each reportable DIBRS incident. Normally, the NCOIC, SFAR, Ops Superintendent, Ops Officer and Commander are granted access as reviewing and approving officials before the data is transmitted. System administrators will ensure all incidents identified under DIBRS reporting criteria are reported through SFMIS.

1.2.7.2. Access to other personnel should be carefully scrutinized to ensure integrity of the system and protection of For Official Use Only (FOUO) information.

1.2.7.3. Users of the system must be made aware of Privacy Act of 1974 requirements and responsibilities, the sensitivity of the information entered into DIBRS, and the requirement to report data only to those who have a need to know in the performance of official duty.

1.2.7.4. Security Forces Unit Responsibility, **Chapter 1**, *Policy and Program Management*, to read: On the first duty day of each month, each Security Forces Administration & Reports Section will perform a computer run of the previous month’s Criminal Summary Report. Once accomplished, the Security Forces Investigations Section will do a comparison with the local AFOSI detachment point of contact to ensure all pertinent criminal activity falling under AFOSI’s Defense Clearance and Investigations Index (DCII) reporting criteria is reported. The NCOIC, SFAR, is responsible to ensure all original AF Forms 3545, *Incident Report*, and criminal DD Forms 1805, *Violations Notice*, are transferred to the local AFOSI detachment and copies are properly filed in the SFAR filing system.

Chapter 2

REPORTABLE DISCIPLINARY INCIDENTS

2.1. Defense Incident-Based Reporting System (DIBRS).

2.1.1. DIBRS is primarily a reporting system covering all active duty military personnel, regardless of service component. Civilian personnel may fall within the reporting requirements of law enforcement under the National Incident –Based Reporting System (NIBRS).

2.1.2. Determination that an incident is reportable under NIBRS simply identifies those incidents and the related data elements that must be forwarded by DMDC to the FBI.

2.1.3. For definitions of reportable incidents, refer to DoD 7730.47-M, *Manual for Defense Incident-Based Reporting System.*

2.1.4. Defense Incident-Based Reporting System (DIBRS), **Chapter 2**, *Reportable Disciplinary Incidents*, to read: The installation security forces commander will ensure all reportable DIBRS incidents, identified in DoD 7730.47-M, Manual for Defense Incident-Based Reporting System, are accomplished using AF Form 3545, *Incident Report.* The AF Form 3545 is the vehicle used to capture the necessary data reportable to the Defense Manpower Data Center (DMDC). No deviation from this procedure is allowed. Incidents not falling within the purview of DIBRS will be documented and reported under existing guidelines.

2.2. National Incident-Based Reporting System (NIBRS).

2.2.1. The NIBRS requirement is comprised of six segments (i.e., Administrative Segment, Offense Segment, Property Segment, Victim Segment, Offender Segment, and Arrestee Segment) and fifty-three data elements.

2.2.2. For military personnel on active duty only, DIBRS adds Commander's Action Segment, Results of Trial Segment, and Corrections Segment. Data elements required for the *Brady Handgun Violence Prevention Ac*t and Victim Witness Assistance reporting are contained throughout all segments. Reporting requirements for civilian offenders are only required by NIBRS.

Chapter 3

CONCEPT OF OPERATION AND SYSTEM REQUIREMENTS

3.1. Concept of Operation.

3.1.1. HQ USAF/XOFX (Plans, Policy, and Programs Division) is the Air Force Office of Primary Responsibility (OPR) for program implementation and budgeting for SFMIS. All budgeting functions are POM'd and coordinated through the 11th WG; Bolling AFB Washington DC. HQ AFCA/FM acts as the paying agent for this effort.

3.1.2. HQ AFSFC/SFOP is the functional lead representative who works with the MAJCOMs, via the Configuration Control Boards (CCB), in the development of the specific requirements for meeting the DIBRS mandate and additional automated data requirements in support of HQ AFSFC managerial concerns and operational needs.

3.1.3. The lead representative works with HQ SSG, Maxwell AFB-Gunter Annex in the development of SFMIS and other automated information system (AIS) requirements. HQ SSG, when necessary, can and does employ contractual assistance in meeting Security Forces requirements.

3.1.4. HQ AFSFC/SFOP serves as the SA for worldwide implementation of the SFMIS.

3.1.4.1. SFMIS operates on the concept of granting permissions and accesses to users of the system at all levels. This is accomplished by using the SA module. HQ AFSFC/SFOP, in conjunction with each MAJCOM POC, identifies an SA at that location. Once identified, the individual will be granted specific accesses and permissions to view data of security forces units under their jurisdiction.

3.1.4.1.1. The MAJCOM SFMIS System Administrator grants specific accesses and permissions to personnel at each one of their assigned security forces units. Note: A MAJCOM will not be able to view any data pertaining to another MAJCOM.

3.1.4.1.2. While HQ AFSFC/SFOP (lead representative) has the capability to view all SFMIS data at all locations worldwide, should it be necessary to provide higher headquarters with any unit or MAJCOM data, MAJCOM notification and coordination will be sought.

3.2. Hardware/Software Requirements.

3.2.1. SFMIS is a web-based product. It uses Netscape as its browser, is password protected, and is Y2K compliant at all levels. SFMIS uses up-to-date, state-of-the art, integrated software to ensure all data is properly encrypted for security concerns and meets full DoD certification and accreditation standards. The SFMIS server is housed at the Defense Information System Agency (DISA) Mega-Center facility at Maxwell AFB-Gunter Annex.

3.2.2. SFMIS requires the Netscape browser to run its application. Netscape can be downloaded free from the web using the following address: "**http.netscape.com/computing/download/index.html**"

3.2.3. For best application performance, it is recommended to use the following hardware:

3.2.3.1. Pentium II 300MHz processor or higher. The higher the MHz the better the performance.

3.2.3.2. 128-MB RAM

3.2.3.3. Windows NT, 95, or 98

3.2.3.4. Netscape v4.61 or higher (can be downloaded free)

3.2.3.5. 5-MB Memory Cache

3.2.3.6. 15-MB Disk Cache (Cache settings can be found by selecting Edit/Preferences/Advanced/Cache in your browser)

NOTE: As technology advances and changes may be necessary to accommodate future data, upgrading of peripherals may also be necessary. Should this occur, MAJCOMs will be advised, with adequate time to respond.

3.2.4. Currently, the SFMIS program encompasses the following modules: Case Reporting, Confinement, System Administration, Password, and Exit. While the current system is not yet fully developed, it is fully functional to report DIBRS data. The second version recently released incorporates Accidents, Tickets, Suspensions, Revocations, Barments, and other reporting capability to the "Case Reporting" Module.

3.3. Security

3.3.1. Users at all levels will be assigned passwords that will grant them access and permissions commensurate with "the right and need to know" information within the system. System administrators at MAJCOM and unit level must continually stress the importance of "Password" security. Passwords will be changed a minimum of once every 90 calendar days. The system possesses the capability to identify the number of days remaining until a change of password is required.

3.3.2. Should a lockout occur as a result of an improper or forgotten password, the MAJCOM or unit SA will take necessary action to assign new passwords.

3.3.3. All SFMIS data is protected by the Privacy Act and must be handled as "FOUO." Known violations of the systems operation or unauthorized dissemination of the "FOUO" information will be immediately reported to the unit or MAJCOM SA, who will notify the commanders at each level of concern.

3.3.4. Commanders at all levels will coordinate with all base functions that may require access to SFMIS information. Normally, Wing/Combat Support Group Commanders, Staff Judge Advocate, AFOSI, and Social Actions Staff require information pertaining to assigned base personnel. Other agencies should be carefully screened for reason of access in which case a local determination can be made. Requests out of the ordinary can be channeled up to HQ AFSFC/SFOP for resolution.

Chapter 4

SYSTEM OPERATION

4.1. Netscape Browser. The requirement for the Netscape browser remains firm. At each version change to Netscape, it is paramount that the latest version be downloaded to affect proper operation of the system. New versions to Netscape will maintain the proper encryption products to preclude violation of privacy information. SFMIS will not work using Internet Explorer as the browser.

4.2. Privacy Information. All information will be strictly controlled in accordance with AFI 33-332, *Air Force Privacy Act Program of 1974*, to ensure only those with officials with a need-to-know have access. Violations of the Privacy Act will be handled by command.

4.2.1. All users of SFMIS must be aware that data displayed on monitors is always susceptible to unauthorized viewing. Take appropriate action to ensure privacy data is always protected.

4.2.2. Protection can be enhanced by installing "time-out" features when the system is not being used, or installing "screen savers" at prescribed time intervals. Your SA's can assist in applying these features.

4.3. Assistance. As SFMIS is an entirely new product for the security forces, HQ SSG will continue to offer assistance for help issues through their Field Assistance Branch (FAB). The FAB provides 24 hour/ 7 day assistance and will troubleshoot Air Force internet, concentrator problems, standard computer systems, local area networking and maintenance issues. They will provide this assistance to Base Network Control Centers, Defense MegaCenters, and functional users worldwide. For any problems encountered, contact the FAB at DSN: 596-5771, or commercial: (334) 416-5771.

4.4. On-Line Manual . The SFMIS program has a fully functioning help manual available to the user. The manuals are designed to be user-friendly, and can be printed out for desk-top reference. Refer to the appropriate DIBRS directive for the DIBRS/NIBRS code tables. These code tables are always subject to change. DMDC controls the additions/deletions and accuracy of the data tables. Any problems being encountered should be up-channeled to HQ AFSFC/SFOP.

4.5. Unresolved Matters. Any issues pertaining to the SFMIS should be directed to HQ AFSFC/SFOP, 1720 Patrick Street, Lackland AFB, TX 78236-5226 for resolution.

ROBERT H. FOGLESONG, Lt Gen, USAF
DCS/Air & Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDD 7730.47, *“Defense Incident-Based Reporting System (DIBRS)”*

DoD 7730.47-M, *“Manual for Defense Incident-Based Reporting System”*

DoDI 7730.47, *“Statistical Report of Criminal Activity and Disciplinary Infractions in the Armed Forces”*.

Section 534,United States Code, “Uniform Federal Crime Reporting Act”.

Sections 10606 and 10607 of Title 42, United States Code, *“Victims Rights and Restitution Act of 1990”*.

Section 922of Title 18, United States Code, “The Brady Handgun Violence Prevention Act”.

AFI 33-332, *“Air Force Privacy Act Program”*.

Attachment 2

IC 2001-1 TO AFI 31-203, SECURITY FORCES MANAGEMENT INFORMATION SYSTEM (SFMIS)

15 AUGUST 2001

SUMMARY OF REVISIONS

This interim change (IC) 2001-1, mandates all security forces units accomplish a monthly computer run within the "Criminal Summary Report" section to identify criminal activity to be reported to the Air Force Office of Special Investigations (AFOSI) for DCII data inputs. It also mandates the use of the AF Form 3545, Incident Report, to document all incidents reportable under the purview of the Defense Incident-Based Reporting System (DIBRS). A star (|) indicates revision from the previous edition.

1.2.7.4. Security Forces Unit Responsibility, **Chapter 1**, *Policy and Program Management*, to read: On the first duty day of each month, each Security Forces Administration & Reports Section will perform a computer run of the previous month's Criminal Summary Report. Once accomplished, the Security Forces Investigations Section will do a comparison with the local AFOSI detachment point of contact to ensure all pertinent criminal activity falling under AFOSI's Defense Clearance and Investigations Index (DCII) reporting criteria is reported. The NCOIC, SFAR, is responsible to ensure all original AF Forms 3545, *Incident Report*, and criminal DD Forms 1805, *Violations Notice*, are transferred to the local AFOSI detachment and copies are properly filed in the SFAR filing system.

2.1.4. Defense Incident-Based Reporting System (DIBRS), **Chapter 2**, *Reportable Disciplinary Incidents*, to read: The installation security forces commander will ensure all reportable DIBRS incidents, identified in DoD 7730.47-M, Manual for Defense Incident-Based Reporting System, are accomplished using AF Form 3545, *Incident Report*. The AF Form 3545 is the vehicle used to capture the necessary data reportable to the Defense Manpower Data Center (DMDC). No deviation from this procedure is allowed. Incidents not falling within the purview of DIBRS will be documented and reported under existing guidelines.